

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**



915-008.014
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: A. Vähä-Sipilä
Serial No.: 0 / 10/667,297 Group No.:
Filed: Sept. 19, 2003 Examiner:
For: Software Integrity Test in a Mobile Telephone

Commissioner of Patents and Trademarks
Washington, D.C. 20231

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country : IB
Application Number : PCT/IB02/04682
Filing Date : November 8, 2002

Reg. No. 31,391

Tel. No. (203) 261-1234

Francis J. Maguire

SIGNATURE OF ATTORNEY

Francis J. Maguire

Type or print name of attorney

WARE, FRESSOLA, VAN DER SLUYS & ADOLPHSON

P.O. Address

755 Main Street, PO Box 224
Monroe CT 06468

NOTE: The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63.

CERTIFICATE OF MAILING (37 CFR 1.8a).

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to the: Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Date: Dec. 19, 2003

Margery B. Hood

(Type or print name of person mailing paper)

Margery B. Hood

(Signature of person mailing paper)

(Transmittal of Certified Copy [5-4])



**WORLD INTELLECTUAL PROPERTY ORGANIZATION
ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE**

34, chemin des Colombettes, Case postale 18, CH-1211 Genève 20 (Suisse)
Téléphone: (41 22) 338 91 11 - e-mail: wipo.mail @ wipo.int. - Fac-similé: (41 22) 733 54 28

**PATENT COOPERATION TREATY (PCT)
TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)**

**CERTIFIED COPY OF THE INTERNATIONAL APPLICATION AS FILED
AND OF ANY CORRECTIONS THERETO**

**COPIE CERTIFIÉE CONFORME DE LA DEMANDE INTERNATIONALE, TELLE QU'ELLE
A ÉTÉ DÉPOSÉE, AINSI QUE DE TOUTES CORRECTIONS Y RELATIVES**

International Application No. }
Demande internationale n° } **PCT/IB02/04682**

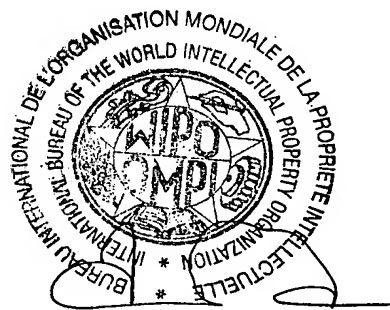
International Filing Date }
Date du dépôt international } **08 November 2002
(08.11.02)**

Geneva/Genève,

**19 September 2003
(19.09.03)**

**International Bureau of the
World Intellectual Property Organization (WIPO)**

**Bureau International de l'Organisation Mondiale
de la Propriété Intellectuelle (OMPI)**



J.-L. Baron

**Head, PCT Receiving Office Section
Chef de la section "office récepteur du PCT"**

PCT REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty

For receiving Office use only	
PCT / IB 0 2 / 0 4 6 8 2	
International Application No.	
08 NOVEMBER 2002	08.11.02
International Filing Date	
INTERNATIONAL BUREAU OF WIPO	
PCT International Application	
Name of receiving Office and "PCT International Application"	
Applicant's or agent's file reference (if desired)(12 characters maximum)	2028421

Box No. I TITLE OF INVENTION	
SOFTWARE INTEGRITY TEST	
Box No. II APPLICANT <input type="checkbox"/> This person is also inventor.	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)	Telephone No.
NOKIA CORPORATION Keilalahdentie 4 FI-02150 ESPOO Finland	Facsimile No.
	Teleprinter No.
	Applicant's registration No. with the Office
State (that is, country) of nationality: Finland	State (that is, country) of residence: Finland
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input checked="" type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)	This person is:
VÄHÄ-SIPILÄ, Antti Kaarlenkatu 13 B 43 FIN-00530 HELSINKI Finland	<input type="checkbox"/> applicant only <input checked="" type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.)
	Applicant's registration No. with the Office
State (that is, country) of nationality: Finland	State (that is, country) of residence: Finland
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
<input type="checkbox"/> Further applicants and/or (further) inventors are indicated on a continuation sheet	
Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE	
The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: <input checked="" type="checkbox"/> agent <input type="checkbox"/> common representative	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)	Telephone No.
AWAPATENT AB Box 45086 SE-104 30 STOCKHOLM SWEDEN	+46 8 440 95 00
	Facsimile No.
	+46 8 440 95 50
	Teleprinter No.
	Agent's registration No. with the Office
<input type="checkbox"/> Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent	

Sheet No. 2

Box No. V	DESIGNATION OF STATES	Mark the applicable check-boxes below; at least one must be marked.
The following designations are hereby made under Rule 4.9(a):		
Regional Patent		
<input checked="" type="checkbox"/> AP	ARIPO Patent: GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Sudan, SL Sierra Leone, SZ Swaziland, TZ United Republic of Tanzania, UG Uganda, ZM Zambia, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT (if other kind of protection or treatment desired, specify on dotted line).....	
<input checked="" type="checkbox"/> EA	Eurasian Patent: AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT	
<input checked="" type="checkbox"/> EP	European Patent: AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, CZ Czech Republic, DE Germany, DK Denmark, EE Estonia, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, SK Slovakia, TR Turkey, and any other State which is a Contracting State of the European Patent Convention and of the PCT	
<input checked="" type="checkbox"/> OA	OAPI Patent: BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, EQ Equatorial Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT (if other kind of protection or treatment desired, specify on dotted line).....	
National Patent (if other kind of protection or treatment desired, specify on dotted line):		
<input checked="" type="checkbox"/> AE	United Arab Emirates	<input checked="" type="checkbox"/> GM
<input checked="" type="checkbox"/> AG	Antigua and Barbuda	<input checked="" type="checkbox"/> HR
<input checked="" type="checkbox"/> AL	Albania	<input checked="" type="checkbox"/> HU
<input checked="" type="checkbox"/> AM	Armenia	<input checked="" type="checkbox"/> ID
<input checked="" type="checkbox"/> AT	Austria +Utility Model	<input checked="" type="checkbox"/> IL
<input checked="" type="checkbox"/> AU	Australia	<input checked="" type="checkbox"/> IN
<input checked="" type="checkbox"/> AZ	Azerbaijan	<input checked="" type="checkbox"/> IS
<input checked="" type="checkbox"/> BA	Bosnia and Herzegovina	<input checked="" type="checkbox"/> JP
<input checked="" type="checkbox"/> BB	Barbados	<input checked="" type="checkbox"/> KE
<input checked="" type="checkbox"/> BG	Bulgaria	<input checked="" type="checkbox"/> KG
<input checked="" type="checkbox"/> BR	Brazil	<input checked="" type="checkbox"/> KP
<input checked="" type="checkbox"/> BY	Belarus	<input checked="" type="checkbox"/> KR
<input checked="" type="checkbox"/> BZ	Belize	<input checked="" type="checkbox"/> KZ
<input checked="" type="checkbox"/> CA	Canada	<input checked="" type="checkbox"/> LC
<input checked="" type="checkbox"/> CH & LI	Switzerland and Liechtenstein	<input checked="" type="checkbox"/> LK
<input checked="" type="checkbox"/> CN	China	<input checked="" type="checkbox"/> LR
<input checked="" type="checkbox"/> CO	Colombia	<input checked="" type="checkbox"/> LS
<input checked="" type="checkbox"/> CR	Costa Rica	<input checked="" type="checkbox"/> LT
<input checked="" type="checkbox"/> CU	Cuba	<input checked="" type="checkbox"/> LU
<input checked="" type="checkbox"/> CZ	Czech Republic +Utility Model	<input checked="" type="checkbox"/> LV
<input checked="" type="checkbox"/> DE	Germany +Utility Model	<input checked="" type="checkbox"/> MA
<input checked="" type="checkbox"/> DK	Denmark +Utility Model	<input checked="" type="checkbox"/> MD
<input checked="" type="checkbox"/> DM	Dominica	<input checked="" type="checkbox"/> MG
<input checked="" type="checkbox"/> DZ	Algeria	<input checked="" type="checkbox"/> MK
<input checked="" type="checkbox"/> EC	Ecuador	<input checked="" type="checkbox"/> MN
<input checked="" type="checkbox"/> EE	Estonia +Utility Model	<input checked="" type="checkbox"/> MW
<input checked="" type="checkbox"/> ES	Spain	<input checked="" type="checkbox"/> MX
<input checked="" type="checkbox"/> FI	Finland +Utility Model	<input checked="" type="checkbox"/> MZ
<input checked="" type="checkbox"/> GB	United Kingdom	<input checked="" type="checkbox"/> NO
<input checked="" type="checkbox"/> GD	Grenada	
<input checked="" type="checkbox"/> GE	Georgia	
<input checked="" type="checkbox"/> GH	Ghana	
<input checked="" type="checkbox"/> NZ	New Zealand	
<input checked="" type="checkbox"/> OM	Oman	
<input checked="" type="checkbox"/> PH	Philippines	
<input checked="" type="checkbox"/> PL	Poland	
<input checked="" type="checkbox"/> PT	Portugal	
<input checked="" type="checkbox"/> RO	Romania	
<input checked="" type="checkbox"/> RU	Russian Federation	
<input checked="" type="checkbox"/> SD	Sudan	
<input checked="" type="checkbox"/> SE	Sweden	
<input checked="" type="checkbox"/> SG	Singapore	
<input checked="" type="checkbox"/> SI	Slovenia	
<input checked="" type="checkbox"/> SK	Slovakia +Utility Model	
<input checked="" type="checkbox"/> SL	Sierra Leone	
<input checked="" type="checkbox"/> TJ	Tajikistan	
<input checked="" type="checkbox"/> TM	Turkmenistan	
<input checked="" type="checkbox"/> TN	Tunisia	
<input checked="" type="checkbox"/> TR	Turkey	
<input checked="" type="checkbox"/> TT	Trinidad and Tobago	
<input checked="" type="checkbox"/> TZ	United Republic of Tanzania	
<input checked="" type="checkbox"/> UA	Ukraine	
<input checked="" type="checkbox"/> UG	Uganda	
<input checked="" type="checkbox"/> US	United States of America	
<input checked="" type="checkbox"/> UZ	Uzbekistan	
<input checked="" type="checkbox"/> VN	Viet Nam	
<input checked="" type="checkbox"/> YU	Yugoslavia	
<input checked="" type="checkbox"/> ZA	South Africa	
<input checked="" type="checkbox"/> ZM	Zambia	
<input checked="" type="checkbox"/> ZW	Zimbabwe	
Check-boxes below reserved for designating States which have become party to the PCT after issuance of this sheet:		
<input checked="" type="checkbox"/> VC, Saint Vincent and the Grenadines	<input checked="" type="checkbox"/> SC, Seychelles	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. (Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)

Form PCT/RO/101 (second sheet) (July 2002)

See Notes to the request form

Sheet No. 3

Box No. VI PRIORITY CLAIM				
The priority of the following earlier application(s) is hereby claimed:				
Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is:		
		national application: country	regional application:* regional Office	international application: receiving Office
item (1)				
item (2)				
item (3)				
item (4)				
item (5)				

☐ Further priority claims are indicated in the Supplemental Box.

The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of this international application is the receiving Office)* identified above as:

☐ all items
 ☐ item (1)
 ☐ item (2)
 ☐ item (3)
 ☐ item (4)
 ☐ item (5)
 ☐ other, see Supplemental Box

* Where the earlier application is an ARIPO application, indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed (Rule 4.10(b)(ii)):

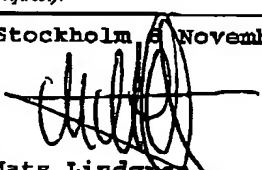
Box No. VII INTERNATIONAL SEARCHING AUTHORITY	
Choice of International Searching Authority (ISA) (if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):	
ISA / <u>EPO</u>	
Request to use results of earlier search; reference to that search (if an earlier search has been carried out by or requested from the International Searching Authority):	
Date (day/month/year)	<div style="display: flex; justify-content: space-between;"> Number Country (or regional Office) </div>

Box No. VIII DECLARATIONS		
The following declarations are contained in Boxes Nos. VIII (i) to (v) (mark the applicable check-boxes below and indicate in the right column the number of each type of declaration):		Number of declarations
<input type="checkbox"/> Box No. VIII (i)	Declaration as to the identity of the inventor	:
<input type="checkbox"/> Box No. VIII (ii)	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	:
<input type="checkbox"/> Box No. VIII (iii)	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	:
<input type="checkbox"/> Box No. VIII (iv)	Declaration of inventorship (only for the purposes of the designation of the United States of America)	:
<input type="checkbox"/> Box No. VIII (v)	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	:

Form PCT/RO/101 (third sheet) (March 2001; reprint July 2002)

See Notes to the request form

Sheet No. 4

Box No. IX CHECK LIST; LANGUAGE OF FILING	
<p>This international application contains:</p> <p>(a) the following number of sheets in paper form:</p> <p>request (including declaration sheets) : 4</p> <p>description (excluding sequence listing part) : 9</p> <p>claims : 3</p> <p>abstract : 1</p> <p>drawings : 3</p> <p>Sub-total number of sheets : 20</p> <p>sequence listing part of description (actual number of sheets if filed in paper form, whether or not also filed in computer readable form; see (b) below) : _____</p> <p>Total number of sheets : _____</p> <p>(b) sequence listing part of description filed in computer readable form</p> <p>(i) <input type="checkbox"/> only (under Section 801(a)(i))</p> <p>(ii) <input type="checkbox"/> in addition to being filed in paper form (under Section 801(a)(ii))</p> <p>Type and number of carriers (diskette, CD-ROM, CD-R or other) on which the sequence listing part is contained (additional copies to be indicated under item 9(ii), in right column): _____</p>	<p>This international application is accompanied by the following item(s) (mark the applicable check-boxes below and indicate in right column the number of each item):</p> <p>1. <input type="checkbox"/> fee calculation sheet : _____</p> <p>2. <input type="checkbox"/> original separate power of attorney : _____</p> <p>3. <input type="checkbox"/> original general power of attorney : _____</p> <p>4. <input checked="" type="checkbox"/> copy of general power of attorney; reference number, if any: <u>GPA 02/0021</u> : _____</p> <p>5. <input type="checkbox"/> statement explaining lack of signature : _____</p> <p>6. <input type="checkbox"/> priority document(s) identified in Box No. VI as item(s): _____</p> <p>7. <input type="checkbox"/> translation of international application into (language): _____</p> <p>8. <input type="checkbox"/> separate indications concerning deposited microorganism or other biological material : _____</p> <p>9. <input type="checkbox"/> sequence listing in computer readable form (indicate also type and number of carriers (diskette, CD-ROM, CD-R or other))</p> <p>(i) <input type="checkbox"/> copy submitted for the purposes of international search under Rule 13ter only (and not as part of the international application) : _____</p> <p>(ii) <input type="checkbox"/> (only where check-box (b)(i) or (b)(ii) is marked in left column) additional copies including, where applicable, the copy for the purposes of international search under Rule 13ter : _____</p> <p>(iii) <input type="checkbox"/> together with relevant statement as to the identity of the copy or copies with the sequence listing part mentioned in left column : _____</p> <p>10. <input type="checkbox"/> other (specify): _____</p>
Figure of the drawings which should accompany the abstract: 1	Language of filing of the international application: English
<p>Box No. X SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE</p> <p>Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).</p> <p>Stockholm 8 November 2002</p> <p></p> <p>Mats Lindgren</p> <p>Authorized Representative</p>	

For receiving Office use only		2. Drawings:
1. Date of actual receipt of the purported international application: 08 NOVEMBER 2002	08. 11. 02	
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:		<input type="checkbox"/> received: <input type="checkbox"/> not received:
4. Date of timely receipt of the required corrections under PCT Article 11(2):		
5. International Searching Authority (if two or more are competent): ISA/	6. <input checked="" type="checkbox"/> Transmittal of search copy delayed until search fee is paid.	

For International Bureau use only	
Date of receipt of the record copy by the International Bureau: _____	

Form PCT/RO/101 (last sheet) (March 2001; reprint July 2002)

See Notes to the request form

SOFTWARE INTEGRITY TEST**TECHNICAL FIELD**

The present invention relates to a method and arrangements for enabling integrity checking of software modules in a mobile communication system software
5 environment.

BACKGROUND

Present day intelligent mobile communication devices have evolved from a first generation of digital mobile telephones that were capable of not much more than
10 conveying voice conversations in real time. Now the devices are capable of communicating in packet switched high speed digital mobile networks and capable of processing and presenting data in much the same manner as a personal computer. The field of use now includes a
15 diverse number of types of applications, among which games and electronic commerce are only two.

Needless to say, in order to provide users of these terminals with suitable software for use in such applications, there is a need for the terminals to be
20 able to download software written by third party software developers as well as the terminal manufacturer. This can be achieved by way of removable memory units on which software modules can be stored. An example of such a removable memory unit is the Multi Media Card (MMC),
25 which has become a standard for many applications in the field of portable intelligent devices.

There is, however, a problem with removable memory units such as a MMC. Because of the fact that the memory unit can be removed from the communication device, it is
30 possible to alter the content, using e.g. a PC, and then

2

re-insert it into the terminal and operate the terminal with modified software. Such alterations may be innocent enough. However, in many situations it is essential that the integrity of the software is maintained from the provider of the software. Needless to say, software relating to, e.g., electronic commerce is of a kind that relies on integrity.

Therefore, there is a need of a system which tests for the integrity of the software before the software is allowed to take control of the communication terminal. In one example of prior art systems, the Symbian system, this is solved by way of storing inside a protected storage area in the terminal, a cryptographic hash of the software that is to be run by processing means in the terminal. Each time the software is to be activated, i.e. run in the terminal, a hash calculation is performed on the software data and if the calculated hash does not match a hash value already stored in the terminal, the software will not be run.

However, this Symbian solution has a drawback in that it is not very flexible when a user of the terminal wish to download additional software applications that have not been subject to the integrity check involving the storage of a hash value in the terminal. Since the additional software has been stored on the removable memory unit by, e.g., a third party, software provider at the time when a user has already obtained the terminal from a terminal provider and the software being intended for use on any terminal, there can be no record of the specific software (i.e. no hash value) in the terminal itself. Therefore, there exist a problem of the software not being allowed to run on the terminal or, as the case may be, can be run only as, e.g., "non-trusted" with less than normal capabilities to operate the terminal.

35

08/11 '02 VEN 14:01 [N° TX/RX 5496]

SUMMARY OF THE INVENTION

It is hence an object of the present invention to provide a solution to a problem related to the lack of flexibility of prior art as indicated above.

5 The object is achieved by way of a method for enabling integrity checking of a software module to be used in a mobile communication terminal according to claim 1 and a mobile communication terminal according to claim 6.

The invention provides a method and a mobile communication terminal for enabling integrity checking of a software module to be used in the terminal. The terminal is capable of communicating in a mobile communication system and the software module is stored on a removable memory unit connected to the terminal. The terminal communicates via the mobile communication system with the software provider. During the communication a digitally signed data block comprising a reference value for use during integrity checking of said software module is received.

20 In some more detail, according to a preferred embodiment of the invention, the method commences by a hashing step during which the software module itself is subject to a hashing step, resulting in a first hash value.

Then is performed transmission of the first hash value as well as a first identifier, which is associated with the memory unit in the form of, e.g., a unit serial number or a software module identification code. A second identifier, which is associated with the terminal in the form of, e.g., a terminal serial number, is also transmitted. The transmission is performed via the mobile communication system to a provider of the software module.

The method continues with the step of receiving, from the provider of the software module, a data block comprising

4

a digital signature and further data. The further data is associated with the memory unit and the terminal and may, e.g., be in the form of the first and the second identifier.

- 5 After the reception of the data block, this is subject to a step of analysis. The analysis comprises a verification of the digital signature and comparison of said further data with said first and second identifiers.

The received data block comprising the signature is then
10 stored, thereby providing a reference value for use during integrity checking of the software module.

In other words, an effect of the invention is that, when a memory unit, such as a MMC card, is inserted to the device, it is "tagged" to the extent that the memory unit
15 is usable only in connection with the terminal in which it was initially connected to. After this "tagging" action, simply copying all software or data that is stored on the card onto another memory unit does not enable another terminal to make full use of the software.
20 That is, the only combination of hardware and software that will result in the device accepting the software is the combination of the unaltered version of the software module, the original memory module and the device with which it was tagged.

25 An advantage of the invention is that it is more flexible than prior art integrity checking solutions where the integrity checking involves use of information that is already stored in a protected storage area of the terminal.

30 Another advantage of the invention is that it allows reliable copy protection of a software module, since a user terminal into which a software module is to be loaded communicates with a provider of the software and, in effect, asks for permission to use the module.

5

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows schematically a block view of a mobile communication system including an embodiment of an mobile communication terminal according to the present invention.

Figure 2 shows a flow chart of an embodiment of a method according to the present invention.

Figure 3 shows a flow chart of an integrity checking procedure.

10 PREFERRED EMBODIMENTS

Below will follow a description of a method for enabling integrity checking according to the present invention. The embodiment is illustrated by way of a schematical view of a communication system 100 in figure 1 and flow charts in figure 2 and 3.

The communication system 100 comprises a mobile communication terminal 101, which includes a number of means for operating the terminal in the system 100. A processing unit 105 is connected via a bus 106 to a removable memory unit 103, an internal memory unit 107, an input/output unit 109 and a radio transceiver unit 115. The input/output unit 109 in turn convey information from a keyboard 111 and a display 113. The radio transceiver unit 115 is capable of establishing a radio connection with a radio base station 119 via an air interface 117 in a radio communication network 121. Information is exchanged between the terminal 101 and a software provider server 125 having a database 127 via a data communication network 123 that is connected to the radio communication network 121.

As the person skilled in the art will realize from the description, the embodiment is one that is implemented on a Symbian platform, which is in use in a number of mobile

6

communication terminals, such as the terminal 101 described above, from a multitude of manufacturers. Moreover, the embodiment of the method utilizes a removable software module, such as the removable memory unit 103 in figure 1, in the form of a Multi Media Card (MMC), also known to the person skilled in the art. However, it shall be stressed that the invention is not limited to implementation in a Symbian system using a MMC card. Other combinations of hardware and software platforms are possible, as the person skilled in the art will realize.

Referring now to figure 1 and 2, when a removable memory card 103 is inserted into a Symbian platform security enabled device, i.e. the terminal 101, a software installation file is executed. The installation software may reside either on the MMC card or in the device itself.

In an initial hashing step 201, the installation function hashes the executables, i.e. the software module, on the MMC card 103 along with the MMC serial number of the MMC card 103.

In an transmission step 203 the installation file sends the international mobile station equipment identity (IMEI) code of the terminal 101, the MMC serial number of the removable memory unit 103 and the hash value resulting from the hashing step 201, via the mobile communication system 100 to the receiving server 125 at the software provider.

Then, in a checking step 205, the software provider checks if it really is the true issuer or provider of a MMC 103 with this MMC serial number, containing the software module corresponding to the first hash value. In other words, it is made sure that the received first hash-value matches a hash value of a software module provided by the provider. If the check is successful, the provider

7

digitally signs the received information and returns the result in a key file to the terminal 101 via the mobile communication system 100.

5 In a storage step 207, the software provider server 125 stores the MMC serial number relationship in its database 127. This will have the effect that the software provider will not sign any other, i.e. later, request for the same MMC serial number and same software module, and thereby "tagging" the software module as discussed above.

10 The key file arrives in a reception step 209 in the mobile communication terminal 101 and is passed on to the software installation software function running in the terminal 101, which is running with full privileges.

15 In a verification step 211 the signature on the key file is verified and a check is made in a checking step 213 that the IMEI code matches the IMEI code of the device. The software installation function also compares, in a comparison step 215, the MMC serial number in the received key file and the MMC serial number of the
20 currently connected MMC card 103.

The signed key file is then stored, in a storage step 217, into the Symbian platform security MMC integrity protection registry, preferably realized in the internal memory 107 of the terminal 101.

25 As a contrast to prior art, where this is done when installing software on the MMC 103, now the software providers software data populates the registry just as if the files had been installed on the MMC 103. But since they are already present there, the only action that is
30 performed is populating the integrity registry.

At this point, integrity checking of the software is enabled. Hence, when starting a program from the MMC 103 a check for integrity can be performed according to,

8

e.g., the following steps, continuing with reference to figure 3.

In a hashing step 301, the platform security system, i.e. Symbian software functions, hashes the target executable.

- 5 It notices that this hash was inserted in this special fashion, and also hashes the MMC serial number of the currently inserted MMC card 103 with the executable.

- 10 In a checking step 303 a check is made whether or not the hash value matches the previously stored hash value in the signed key file. A check is also made whether the MMC identifier matches the stored signed identifier in the key file. If the values match, the executable code is allowed to run on the terminal 101, as indicated by the execution step 305.

- 15 The invention as described above provides a simple and effective way of enabling integrity check of a software module. For example, if the software module stored in the removable memory unit 103, e.g. a MMC, has been copied onto another MMC and that other MMC is inserted to a
20 terminal 101 that has been tagged with the original MMC, it's unique MMC serial number is not the same. Hash verification fails and the software module will not be allowed to run.

- Also, if the MMC is connected to a second terminal (not
25 shown) after it has been "tagged" when initially connected to a first terminal 101, the software provider will not sign the request for a signed key file.

- Also, if the MMC is copied before "tagging" it, the MMC serial number of the card that it has been copied onto
30 (not shown) is not in the software provider server database 127 of sold cards, so the software provider will not honour the MMC serial number.

Also, if a "software pirate" is producing a plurality of cards (not shown) with one and the same MMC serial

9

number, only the first "tagging" request is honoured by the software provider.

Finally, the signed reply from the software provider (the tagging message, i.e. the key file) cannot be forged
5 because it contains the IMEI of the target mobile terminal and is signed by the software provider.

08/11 '02 VEN 14:01 [N° TX/RX 5496]

10

CLAIMS

1. A method for enabling integrity checking of a software module to be used in a mobile communication terminal, said terminal capable of communicating in a mobile communication system, said software module being stored on a removable memory unit connected to the terminal, said method characterized in that the terminal communicates via the mobile communication system with the software provider, said communication including reception of a digitally signed data block comprising a reference value for use during integrity checking of said software module.
2. A method according to claim 1, comprising the steps of:
- hashing the software module, resulting in a first hash value,
 - transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal and the first hash value via the mobile communication system to a provider of the software module,
 - receiving, from the provider of the software module, a data block comprising a digital signature and further data associated with the memory unit and the terminal,
 - analysing the received data block, comprising verification of the digital signature and comparison of said further data with said first and second identifiers,
 - storing the received data block comprising the digital signature, thereby providing a reference value for use during integrity checking of said software module.
3. A method according to claim 2, where the transmission of the first identifier includes transmission of a memory unit serial number.

11

4. A method according to claim 2, where the transmission of the first identifier includes transmission of a software module identification number.
5. A method according to any one of claims 2-4, where the transmission of the second identifier includes transmission of an international mobile station equipment identity code.
6. A mobile communication terminal, comprising means for enabling integrity checking of a software module to be used in the terminal, said terminal capable of communicating in a mobile communication system, said software module being stored on a removable memory unit connected to the terminal, said terminal characterized in that it comprises means for communicating via the mobile communication system with the software provider, said means for communication including means for receiving a digitally signed data block comprising a reference value for use in means for integrity checking of said software module.
7. A terminal according to claim 6, comprising:
- means for hashing the software module, arranged to provide a first hash value,
 - means for transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal and the first hash value via the mobile communication system to a provider of the software module,
 - means for receiving, from the provider of the software module, a data block comprising a digital signature and further data associated with the memory unit and the terminal,
 - means for analysing the received data block, comprising means for verification of the digital signature and comparison of said further data with said first and second identifiers,

12

- means for storing the received data block comprising the digital signature, arranged to provide a reference value for use during integrity checking of said software module.

- 5 8. A terminal according to claim 7, where the means for transmitting the first identifier includes means for transmitting a memory unit serial number.
9. A terminal according to claim 7, where the means for transmitting the first identifier includes means for
- 10 transmitting a software module identification number.
10. A terminal according to any one of claims 7-9, where the means for transmitting the second identifier includes means for transmitting an international mobile station equipment identity code.

15

13

ABSTRACT

Integrity checking of a software module to be used in a mobile communication terminal (101) is illustrated. The terminal (101) is capable of communicating in a mobile communication system (100) and the software module is stored on a removable memory unit (103) connected to the terminal (101). The terminal (101) communicates via the mobile communication system (100) with the software provider (125). During the communication a digitally signed data block comprising a reference value for use during integrity checking of said software module is received.

Figure 1 for publication

15

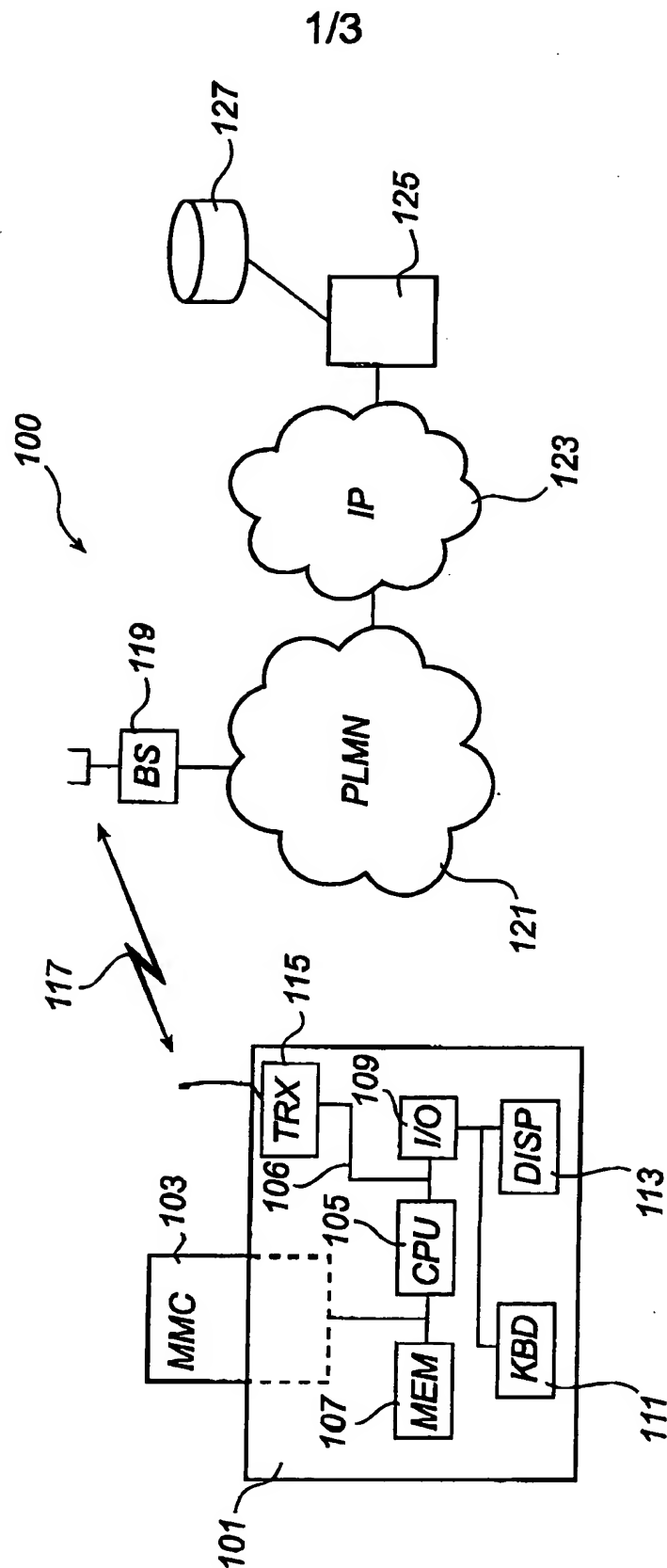
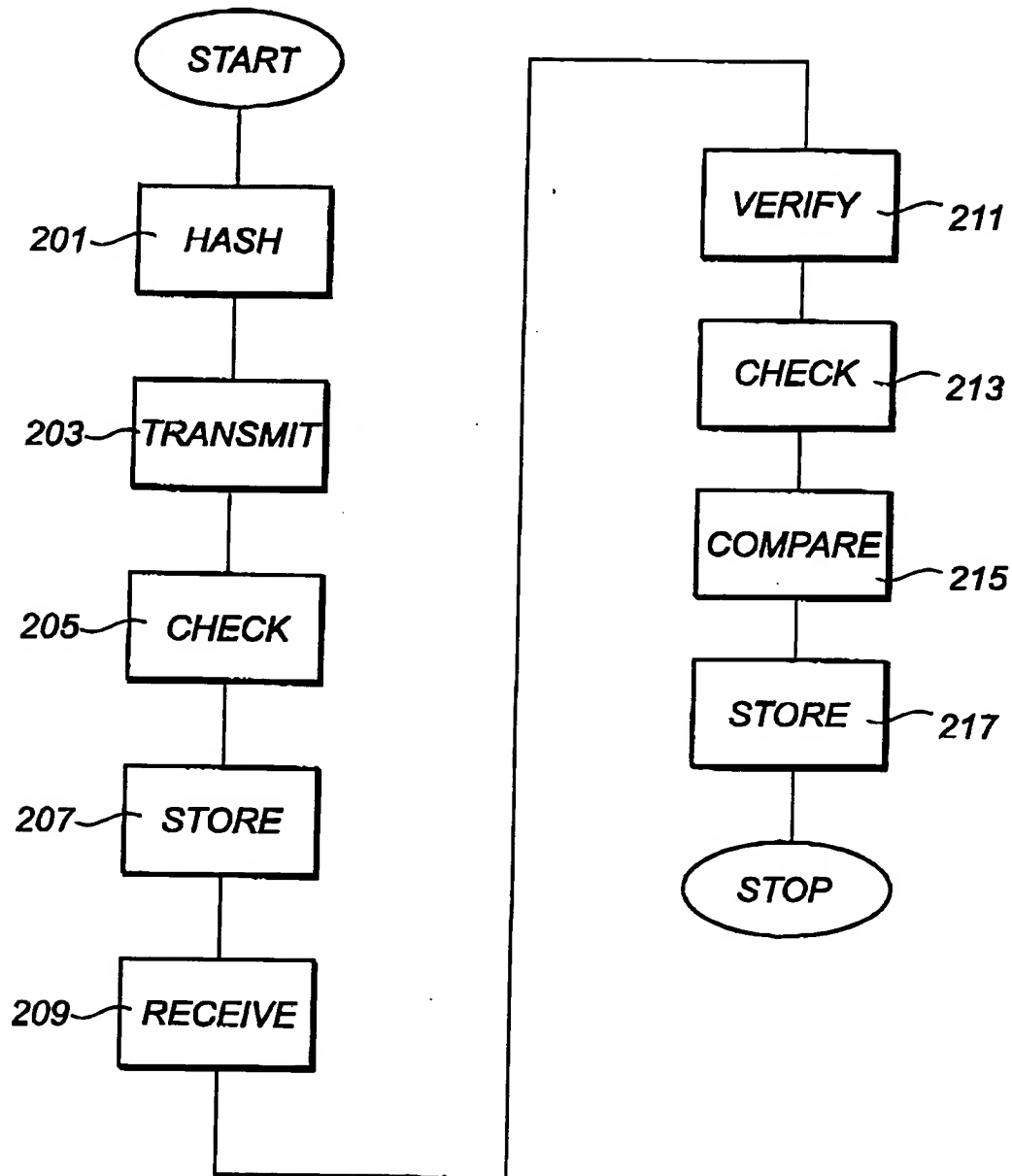
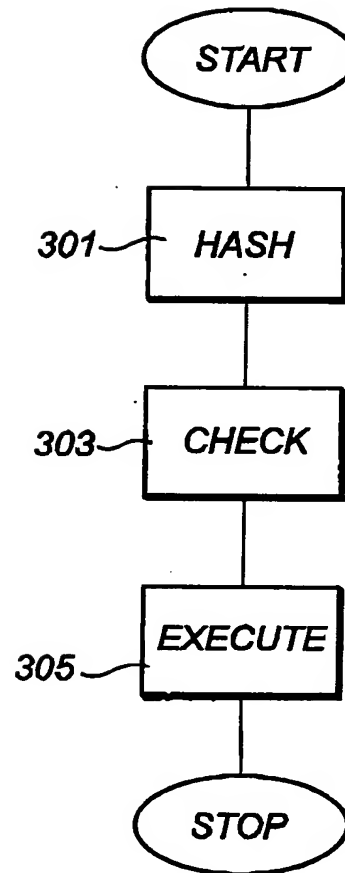


Fig. 1

2/3

*Fig. 2*

3/3

*Fig. 3*